Chapter 23 - Custody and Accountability

2301 Custody of Classified Information

Any person who has possession of, or is charged with responsibility for, classified information must protect and account for that information. The following measures shall be applied to properly protect classified information.

A. While in use, classified information (i.e., documents, disks, etc.) shall be kept under continuous observation. Classified information shall not be left unattended.

B. An office that receives classified information (in any form) and has no authorized storage equipment available must either return the classified information to the sender, arrange with another office to properly store the information, or destroy it by an approved method. Under no circumstances shall classified information be left unattended, in an unauthorized storage container, or in the custody of a person who does not have the proper security clearance and an established need-to-know.

C. Classified information must be delivered to, or left in the custody of, individuals who have the appropriate level security clearance and need-to-know.

D. Custodians of classified information must ensure that persons who do not possess an appropriate security clearance and need-to-know, assigned to or visiting an office, do not take or read classified information, overhear classified conversations, or have visual access to classified information. Classified information must not be placed or displayed in a manner where it can be seen through a window or a doorway.

E. Classified information must be discussed only with those individuals who possess the appropriate security clearance and need-to-know. Classified information shall not be discussed in public or other places where unauthorized persons could overhear it.

F. Classified information must not be checked with baggage or left in a private residence, vehicles, hotel rooms and safes, aircraft, train compartments, buses, public lockers, or other locations where the information could be compromised.

G. Classified information should not be opened, read, studied, displayed, used, or discussed in any manner in

a public conveyance or place. Classified information must be appropriately stored in a GSA-approved security container at all times when not in use.

H. Classified information must be covered with the appropriate level GSA Standard Form cover sheet (SF-703, SF-704, or SF-705).

2302 Custody During Emergencies

A. In the event of fire, natural disaster, civil disturbance, or an evacuation of office space, classified information shall be protected by removing it under secure means, by placing it in locked storage cabinets or safes, or by proper destruction. Persons who are away from their offices and have classified information in their possession at the time shall properly safeguard such information.

B. The head of each operating unit or departmental office shall prepare a general plan for the emergency protection and destruction of classified information. The plan is vital in overseas locations and in locations where a potential threat to a Government facility exists. The plan shall include:

1. The location and identity of the information to be destroyed; and

2. The priority for destruction, persons responsible for destruction, and the recommended place and method of destruction.

C. The classified destruction plan shall be distributed to all cleared personnel working with classified information. The security contact shall ensure that personnel are briefed on the responsibilities of the plan.

2303 Relocating Containers Housing Classified Information

When classified information is physically moved from one office or facility to another, it must be retained in a locked, approved security container. Supervisors or programs managers responsible for control of the security container must notify the servicing security officer prior to relocating a security container so the security officer can note the new location of the container. The custodian or other cleared personnel must maintain constant supervision of the container during the move. The servicing security officer or security contact is responsible for notifying the Classified Control Point (CCP) on the new location of the container when this information is maintained in an electronic database. The data is necessary to be able to track all changes. The servicing security officer or security contact must also annotate any changes to the relocation of the security container

on the SF-700, Security Container Information form.

2304 Accountability of Classified Information

The head of an operating unit, in coordination with their servicing security officer or security contact, shall establish procedures for the accountability of Top Secret, Secret, and Confidential information. All Top Secret and Secret information shall be properly controlled and accounted for by use of written records or an electronic database. In order to control and account for classified information electronically, each operating unit shall designate an office/unit Classified Control Point. The head of an operating unit may request an exception to this policy from the Director for Security. Procedures shall ensure that the movement of classified information can be traced, dissemination is limited, prompt retrieval of information can be obtained, the loss of information can be detected, and excessive holdings and reproduction are limited.

A. Top Secret and Secret Information.

1. The head of an operating unit shall appoint an appropriately cleared employee to serve as the Top Secret and Secret control officer within his or her operating unit. The appointment shall be made in writing with a copy forwarded to the servicing security officer. The Top Secret and Secret control officers are responsible for receiving, dispatching, and maintaining control and accountability of Top Secret or Secret information, respectively, within their unit. The head of an operating unit may appoint one individual to serve as both the Top Secret and the Secret control officer provided the individual has a Top Secret security clearance; otherwise, the head of an operating unit must appoint two individuals cleared at the appropriate level.

2. Top Secret or Secret information shall be controlled and inventoried using either an electronic accountability registry system, where available, or the operating unit's accountability register, Classified Document Control Record, CD-481. Information annotated on the accountability register shall be unclassified. If the description of the document is classified, then the register shall identify the control number of the document, total page numbers, copy number, originator, and other pertinent information in order to differentiate this document from other documents. When a Top Secret or Secret document is routed internally within the Department, the Top Secret or the Secret control officer, in coordination with the designated CCP, shall trace the movement of the document by electronic means. If the Top Secret or Secret document is transmitted outside of the Department, a document receipt form, CD-76, or electronic version of a classified document receipt shall be prepared by the transferring unit and signed by the new recipient upon receipt of the classified information.

3. The Top Secret document shall be covered (in addition to the SF-703) with a Top Secret Disclosure

Register, Form CD-74, to identify each recipient who has been given access to the document. The name and title of all individuals, including support personnel, to whom information in the document has been disclosed, shall be recorded along with the date of disclosure. The Form CD-74 shall remain attached to the document until the document is downgraded, transmitted outside of the Department, or destroyed.

4. The Secret document shall be covered (in addition to the SF-704) with a Classified Material Receipt Form, CD-76, to identify each recipient who has been given access to the document. The name and title of all individuals, including support personnel, to whom information in the document has been disclosed, shall be recorded along with the date of disclosure. The CD-76 shall remain attached to the document until the document is downgraded, transmitted outside of the Department, or destroyed.

5. When a Top Secret or a Secret document is routed internally within the Department, the Top Secret or the Secret control officer, in coordination with the designated Classified Control Point (CCP), shall track the movement of the document by electronic means. If a Top Secret or Secret document is transmitted outside the Department, a document receipt form shall be prepared by the transferring CCP. The CCP shall maintain a suspense copy of all document receipts for classified material transferred outside the Department. If a signed receipt is not received within 30 days, then a follow-up receipt shall be mailed to the organization that received the mailed document. If a signed receipt is still not received within another 30 days, then the CCP shall contact the organization to determine the status of the classified material

6. Top Secret and Secret control officers shall inventory Top Secret and Secret documents on an annual basis and more frequently where circumstances warrant. Each document must be visually inspected to ensure that the document is complete or accounted for by written evidence of proper disposition. The results of this inventory shall be forwarded to the Office of Security through the security contact or servicing security officer.

7. Reproduction of Top Secret or Secret information, or portions of documents containing Top Secret or Secret information, shall not occur without the consent of the originator. The number of copies of documents containing Top Secret information shall be kept to an absolute minimum. Records of reproduced Top Secret or Secret documents shall be maintained to indicate the number of copies made and their distribution. Each additional copy shall be assigned a separate control number and recorded in the electronic or written database system. The accountability register shall be annotated with the additional copies and control numbers. The SF-703 or SF-702 and CD-74 or CD-76 forms shall be attached to each duplicate copy.

8.Top Secret and Secret documents shall be retained only to satisfy current operational requirements. Documents that have not been destroyed shall, when appropriate, be downgraded, declassified, or archived to designated records centers. The Departmental Records Management Office will be consulted for guidance on the retention and archiving of classified records.

9. The CD-481 form or a receipt for Top Secret or Secret documents generated by an electronic system shall be used each time a document is transmitted from one individual, division, office, operating unit, or agency to another.

10. In accordance with existing records control schedules, the Classified Material Receipt, CD-76, shall be retained by the office or operating unit for a period of at least two years. The Top Secret Control Register, CD-73, shall be retained for a period of five years after the related document is downgraded, transferred, or destroyed. The Top Secret Disclosure Record, CD-74, shall be destroyed when the related document is downgraded, transferred, or destroyed. Upon completion of the appropriate retention period, the record may be destroyed in accordance with paragraph 2307 below.

B. Confidential Information.

1. Confidential information must be protected from unauthorized disclosure and may be controlled as prescribed above at the option of the head of an operating unit or if the sender deems it necessary. Confidential materials which bear special dissemination and reproduction controls must be transmitted using the Classified Material Receipt, CD-76, shall be receipted for each transmission.

2. The CD-76 shall be retained by the office or operating unit for a period of at least two years after which it may be destroyed in accordance with paragraph 2307 below.

C. Classified Material Receipt Areas. The head of each operating unit responsible for protecting classified information shall develop and implement procedures to protect incoming mail, bulk shipments, and items delivered by messenger that contain classified material. Procedures shall be established at receipt points to limit access to classified information to cleared personnel only.

D. Clearance Rosters. Each servicing security officer and security contact shall maintain a current list of employees and other personnel associated with the operating unit who are cleared and authorized to receive Top Secret, Secret, and Confidential information. In addition, the security officer and security contact will maintain a list of persons outside the Federal Government who may be authorized to receive classified material

from the operating unit. Such lists will be available for security inspection and assistance reviews by the Office of Security.

2305 Annual Inventory and Disposal of Classified Holdings

Offices maintaining classified information must conduct an annual inventory and review their classified holdings to reduce the amount necessary for operational and program purposes. All classified documents shall be reviewed upon initial receipt and during the annual inventory. The inventory shall include a review to determine possible downgrade, declassification, or destruction of classified holdings. At a minimum the electronic tracking system will perform the following functions:

- Describe the information to include the originator, classification level, subject, date of information, and number of copies;
- Track internal routing; and
- Identify disposition, by transmission outside the office or organization, by transfer to a storage area, or by destruction.

2306 Working Papers

Working papers are drafts, notes, photographs, etc., in paper or electronic form that are accumulated or created to assist in the formulation and preparation of a finished document. Working papers that contain classified information must be:

- Dated when created;
- Marked with the highest classification of the information which they contain;
- Portion marked;
- Protected in accordance with the highest classification;
- Accounted for, controlled, and marked in the manner prescribed for a finished document of comparable classification when: 1) transmitted in any way; 2) permanently filed; or 3) retained for more than 180 days from date of origin; and
- Destroyed when no longer needed.

2307 Destruction of Classified Material

A. Authorized Destruction. When no longer needed, classified documents shall be destroyed in a manner

sufficient to preclude recognition or reconstruction of the classified information. The head of each operating unit, in consultation with the servicing security officer, shall establish procedures for the proper destruction of classified information in the organization. Such procedures must ensure that adequate destruction records are maintained, authorized destruction methods are used, information is protected during transport, and the destruction is properly witnessed. Classified documents may be destroyed by one of the following methods.

1. **Shredding.** Only GSA-approved shredders shall be used for destruction of Top Secret, Secret, and Confidential information. Top Secret material must be destroyed through the use of a crosscut shredder that turns the material into powder form. Secret and Confidential material may be destroyed by a crosscut shredder that renders the material in strips that do not exceed 1/32" in width and 3/8" in length. Material shredded to these specifications needs no further destruction. Only equipment listed on the GSA Federal Supply Schedule shall be used as approved security destruction devices. Shredders used for destroying classified material shall be properly marked with appropriate signage to identify its classified usage. The signage shall clearly identify the highest level of classified information that is authorized for destruction by the shredder. If uncertain, individuals should check with their security contact or servicing security officer to verify the authorized level of destruction of the equipment.

2. **Burning.** Classified documents shall be placed in burn bags marked as "Classified Waste Only." The destruction of Top Secret and Secret documents shall be witnessed and recorded in the electronic database or on Form CD-481, Classified Document Control Record, before they are placed in the burn bag. A complete chain-of-custody shall be used from the moment classified materials are placed into a burn bag until the moment the burn bag contents are properly and completely destroyed. A classified material receipt shall be used to document the transfer of burn bags. Each person having access to the burn bags shall possess the necessary clearance. Documents shall be burned completely. Unburned residue cannot be allowed to remain or escape by wind or draft.

3. **Other Methods of Destruction**. Written approval shall be obtained from the Office of Security before other methods of destruction such as melting, chemical decomposition, or mutilation are used to destroy classified material.

B. Storing and Transporting Material for Destruction. Classified material awaiting destruction shall be stored in an approved storage container. Individuals transporting containers containing classified waste material must provide adequate safeguards to prevent unauthorized disclosure of the information. Such containers must not be left unsecured or unattended when being transported to an authorized destruction site.

C. Records of Destruction. Records of destruction are required for Top Secret and Secret information. The record of destruction shall include an unclassified description of the material, the date of actual destruction, and signatures of the destroyer of the material and the individual who witnessed the destruction. Destruction records shall be retained at least five years for Top Secret information and two years for Secret information. Holders of boxes or burn bags containing classified information marked for destruction must attach a classified material receipt when transferring the material to another individual for destruction. Each burn bag shall be clearly marked with the following identifying data:

1. Operating unit;

2. Bag number; and

3. Name of person responsible for the contents of the burn bag.

Example in the transfer of three burn bags:

NTIA, bag 1 of 3, bag 2 of 3, and bag 3 of 3; T. Jones.

D. Classified Waste. Classified waste material (in any form) shall be appropriately protected at all times. Classified waste is defined as notes (working papers), carbon paper, typewriter and printer ribbons, disks and other information containing classified information. Binders, paperclips, cartridges, etc. must be removed before classified material to be destroyed is placed in burn bags. See destruction methods in paragraph 2307 A. above.

E. Destruction of Information Technology Material and Equipment. Guidance on the destruction of classified waste resulting from processing on information technology systems, such as personal computer and printers, can be obtained from the IT Security Manual, Office of the Chief Information Officer.

2308 End-of-Day Security Check

A. The head of each operating unit or departmental office, in consultation with the servicing security officer, shall establish a system of security checks at the close of each working day to ensure that the following conditions are met.

1. All classified information has been returned to the appropriate GSA-approved security container and is properly stored;

2. All typewriter ribbons, floppy disks, carbons, removable PC hard drives, and working materials that contain classified information are properly stored in an appropriate GSA-approved security container;

3. Classified waste is properly stored or destroyed;

4. Wastebaskets and recycle containers do not contain classified material;

5. All security containers are double-checked to ensure that they are locked;

6. All doors and windows to the area are locked;

7. Cryptographic ignition keys (CIKs) are removed from security telephone equipment and properly safeguarded;

8. Alarms (if in place) are properly activated; and

9. The Security Container Check Sheet, SF-702, is completed in accordance with paragraph 2407 of the Security Manual.

B. The Activity Security Checklist, SF-701, shall be used to indicate that an end-of-day security check has been conducted every day that the office was occupied for duty purposes. The SF-701 shall be displayed and affixed to, or immediately adjacent to, the office exit door. The responsibility for the end-of-day security check shall be placed on the last employee to depart the office area. Individuals responsible for conducting the end-of-day security check must thoroughly check the entire work area where classified information is processed, handled, discussed, and stored, and then sign and date the SF-701. Supervisors are responsible for establishing procedures in the office area to ensure these requirements are met. The originating office should retain each completed SF-701 for 90 days.

2309 Copier Security

A. Introduction. This paragraph outlines the security precautions necessary to protect classified and other sensitive information from possible compromise as a result of copier use or other duplicating means. New technology available for copiers increases security vulnerabilities. The term copier refers to reprographics machines, facsimile machines, printers that produce hard copy output, electronic blackboards that provide a

reproduction of what is written on the board, and any machine with a combination of these functions.

B. Security Threats. Security measures shall address the following situations.

1. Individuals who may attempt to gain unauthorized copies of classified material;

2. The misuse of copiers by authorized persons; and

3. The technical hazard of information retention through latent or residual images on the machines or electronic memory.

C. Designation of Copiers for Classified and Unclassified Reproduction.

1. Reproduction machines within the Department shall be designated as "approved" or "non-approved" for the reproduction of classified information, if they are located at a site that contains both classified and unclassified information. The servicing security officer is designated to authorize copiers within his/her organization. Determination of approved copiers shall be based upon the following:

a. **Physical Location of the Copiers.** Approved machines shall be located in locked or secured areas to deny access to unauthorized users. If no locked or secure area is available, the copier shall be located away from high traffic areas where unauthorized persons are situated. The location shall allow continuous monitoring by office personnel of the copier during work hours.

b. **Equipment Design.** All machines used for classified reproduction shall be approved for classified usage. These machines have few known security hazards and possess the most security design features (i.e., lock, key pad, and copy counter). It is recommended that copiers utilized for reproduction of classified information be equipped with removable hard drives. Machines designed with remote diagnostic capabilities shall not be used to reproduce classified material. Those machines that contain memory capabilities shall have the memory removed by an authorized person prior to servicing by non-cleared personnel.

2. After designation of a copier as "approved" or "non-approved," it will be clearly identified by a posted notice. Additionally, security officers will issue classified reprographics equipment approval letters to the office managers possessing these machines. The letter will identify the machine(s) that are approved, the location, and the point-of-contact in the office. The point-of-contact will be required to coordinate with

the servicing security officer when potential security problems arise, or when there are incidents of possible compromise.

D. Approval. Reproduction of classified material shall be limited to those instances when it is absolutely necessary. Confidential and Secret information may be reproduced without prior approval of the originator unless otherwise indicated on the document. When Top Secret or Secret material is reproduced, the additional copies must be introduced into the written (CD-481) or electronic accountability system. Reproduction of Top Secret material requires coordination with the originator and the Top Secret Control Officer. Some sensitive unclassified information may require approval of the originator prior to reproduction.

E. Accountability/Control Logs. Records must be maintained to show the number and distribution of all reproduced Top Secret documents, special access documents, and those Secret or Confidential documents which bear special dissemination and reproduction limitations. Classified copier control logs are recommended, but are not required for other Secret or Confidential material. If used, these logs should record the identity of the individual making the copies, a description of the document(s), the originator, the number of copies made, and the date and time of reproduction. Reproductions of all Top Secret and Secret documents must be accounted for and controlled.

F. Copier Security Procedures. The following procedures shall be followed when reproducing classified information.

1. Cleared individuals will remain at the copier until classified reproduction is complete.

2. Digital copiers with electronic chip memory capabilities shall be utilized only in a stand-alone capacity. Digital copiers used to reproduce classified information shall not be connected to any network or telephone line.

3. For older copiers, after reproduction of classified material, each individual copying the material shall run a specially designed copy paper through the copier (at least three to five times) to alleviate latent images from being retained on the equipment=s drum (a copy of this specially designed paper can be obtained from the servicing security officer or the Office of Security).

4. Before leaving the copier, individuals must check the copier for any copies or originals that may be left in the copier.

5. Classified waste, such as rejected copies or blank copies run after classified material is processed, must be destroyed in accordance with paragraph 2307 of the Security Manual.

6. If the copier malfunctions and the copier cannot be cleared or the copies cannot be retrieved, the servicing security officer shall be notified to ensure that the copier is removed from approved service until the supervising office manager certifies that the malfunction has been properly cleared, at which time, the copier may be re-certified for classified usage.

G. Scheduled Maintenance. The servicing security officer or security contact shall be notified of the scheduled service visit and arrange for an appropriately cleared employee to be present. Any documents, image retaining drum sheets, or memory chips removed from the machine shall be collected by the cleared employee and turned over to the servicing security officer. No unescorted maintenance person shall be allowed access to any reproduction equipment used for the reproduction of classified materials.

2310 Mail Processing Facilities

The supervisor of a mailroom shall develop procedures to protect classified information that may be contained in incoming mail, bulk shipments, or items delivered by messenger. Such procedures must limit access to classified information to appropriately cleared personnel only. U.S. Postal Service first class, certified, and registered mail should be presumed to contain classified information. Unless a mailroom has cleared personnel authorized to accept and open mail that may contain classified information, all in-coming mail, bulk shipments, and items delivered by messenger must be forwarded directly to the individual addressed on the envelope. In addition, supervisors of mailrooms must establish measures to screen and/or x-ray incoming mail, bulk shipments, or items delivered by messenger if necessary. Mailroom supervisors should coordinate these measures with their servicing security officer.